

CLAIMS

1. A method for discovering a trust chain, at least comprising attribute delegations each
 5 with an issuer and a subject, that overall imparts a required attribute to a subject and is
 grounded in a known trusted issuer, the method involving the use of certificates as
 justification of associated attribute delegations and comprising the steps of:

- a) - setting as a primary goal to be proved an attribute delegation from a known trusted
 issuer to said subject;
- 10 b) - seeking a backwards proof of said primary goal by a process of recursively taking a
 goal to be proved, starting with said primary goal, and decomposing it into subgoals
 one of which corresponds to an attribute delegation that is justified by an available
 certificate and has the same subject as the goal being decomposed, inability to
 decompose a subgoal that has not been proved causing the process to backtrack to a
 15 previous subgoal to seek a new decomposition of the latter;
- c) - determining that a trust chain has been found upon the process of step (b) producing
 a chain of subgoals proved by corresponding certificates, that grounds in a subgoal
 justified by a justified attribute delegation that has as issuer the said known trusted
 issuer included in said primary goal.

20

2. A method according to claim 1, wherein the known trusted issuer included in said
 primary goal is a specifically identified entity that is inherently trusted by the discovery
 method at least in relation to said required attribute, said justified attribute delegation of
 step (c) being an attribute delegation that is justified by a corresponding certificate.

25

a 3. A method according to ^{Claim 1}~~claim 1~~, wherein the known trusted issuer included in said
 primary goal is the discovery method itself; said justified attribute delegation of step (c)
 being an attribute delegation that is justified either by an axiom inherently trusted by the
 discovery method, or by a corresponding certificate.

30

5. A method according to claim 1, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, step (b) involving decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

Claim 1

Claim 1

Claim 1

ite before allowing
Claim
y one of claims 1 t

~~any one of claim~~